

DDoS攻撃事案共通様式

西暦で記載

2026 年 10 月 10 日
20 時 40 分

24時表記で記載

宛先は変更不要

(報告先機関の長) 殿

【重要】各シートは削除しないこと
セルが黄色になる場合は入力エラーのため修正すること

以下の報告根拠に基づき、別添のとおり報告いたします。

以下ページに記載されている本様式の対象となる手続等(一覧)から選択し記載
<https://www.cyber.go.jp/policy/group/cyber/policy.html>

報告根拠:

☒ 法令等に基づく報告 (「本様式の対象となる手続等」から該当手続名を記載すること。)

●●業法第XX条

☐ 上記選択肢以外 (自主判断による情報提供を目的とした任意報告等)

※任意報告の同報先がある場合は、以下に同報先機関を記載すること。

【報告の区分】

(1) 報告の版: 第 2 報

(2) 速報/続報/詳報の別:

☐ 速報(新規) ☒ 続報 ☐ 詳報(確報)

(前回報告: 2026 年 10 月 5 日 13 時 30 分)

(受付番号※: 000000000000)

前回報告は1つ前の報告
の

※個人情報保護委員会より通知されている場合

本様式に記載
国家サイバー統
止のため、注意

受付番号(12桁)は、個人情報保護委員会へ報告する場合、且つ、続報の時のみ受付完了メールを確認して記載 (例)
123456789012

官房
国防

記載内容の全部又は一部について、内閣官房国家サイバー統括室との共有等を希望しない場合は、その旨及び共有等を希望しない内容について以下に記載してください。

☐ 内閣官房国家サイバー統括室への共有等を希望しない

共有等を希望しない場合はチェック

共有等を希望しない内容:

共有等を希望しない場合は必ず共有を希望しない内容を記載

(注) 重要電子計算機に対する不正な行為による被害の防止に関する法律第5条に基づく報告である場合は、「共有等を希望しない」とした場合でも、同法に基づき内閣官房国家サイバー統括室等に情報提供されることがあります。

(注) 報告を行う者が、重要インフラのサイバーセキュリティに係る行動計画(2022年6月17日サイバーセキュリティ戦略本部決定)に定める重要インフラ事業者等である場合は、同行動計画に基づき、「共有等を希望しない」とした場合でも、内閣官房国家サイバー統括室に共有されることがあります。

1. 記載の手引き

(1) 本様式の対象となる手続等

報告根拠に記載する法令、ガイドライン等(重要インフラのサイバーセキュリティに係る行動計画において重要インフラ分野として指定されている分野の法令、ガイドライン等を含む)については、次のウェブサイトに記載。ただし、具体的な提出先や提出方法、追加的な報告事項の有無については、各法令、ガイドラインや、各省庁が公表する方法に従うこと。また、業法等の固有の報告項目については、様式本体の「6. その他特記事項」に記載すること。このほか、警察への相談を行う場合や、その他所管省庁から本様式により報告を行うよう要請等があった場合についても、本様式を利用することができる。

<https://www.cyber.go.jp/policy/group/cyber/policy.html>

(2) 記載事項

報告をしようとする時点で把握している範囲で、1から6までの内容を記載してください。また、続報として提出する場合には、前回の報告から記載を変更した箇所に下線を引くなど、変更箇所が分かるようにしてください。

業種・業種番号(数字4桁)は日本標準産業分類※から記載。業種が複数ある場合は、メインの業種について記載。
※日本標準産業分類:「政府統計の総合窓口(e-Stat)」(https://www.e-

1. 報告者の概要

報告者の氏名 又は名称	(フリガナ)	マルマルカブシキガイシャ		
		〇〇株式会社		
(氏名は旧姓での記載を可とする)				
法人番号(13桁)		1234567890123		
業種・業種番号		××業	0000	
報告者の住所 又は居所		〒000-0000 □□県△△町1-2-3		
代表者の氏名 (報告者が法人等の 場合に限る。)	(フリガナ)	ナйкаク ゴシチノキリ		
		内閣 五七桐		
(氏名は旧姓での記載を可とする)				
事務連絡者の氏名	(フリガナ)	ナйкаク サクラ		
		内閣 桜		
	(氏名は旧姓での記載を可とする)			
	所属部署	サイバー総括部	電話番号	000-1111-2222
	E-mail	ELPMAXE@EXAMPLE.JP		

2. 事案の概要(業務への影響)

(1) 事案の概要

西暦で記載

24時表記で記載

発生日時: 2026 年 10 月 5 日 10 時 0 分
発覚日時: 2026 年 10 月 5 日 10 時 10 分

事案の発生日時、発覚日時を記載(確定していない場合や不明な場合は、可能性の高い発生日時、発覚日時を記載した上で、枠

〇〇株式会社が運営する入会登録HP (https://...../)

- ・10月5日に入会登録HPにおいて、1分間に約10万件の入会登録申請があり、HPがつながりにくい状況が発生
- ・10月10日に当該HPに1分間に約15万件の入会登録申請があり、前回と同様にHPがつながりにくい状況が発生

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

(2) 重要インフラサービス維持レベルについて(重要インフラのサイバーセキュリティに係る行動計画(2022年6月17日サイバーセキュリティ戦略本部決定)に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。)

・重要インフラサービスのサービス維持レベルの逸脱の有無:

☐ 有 ☒ 無

・他の事業者等への波及の可能性:

☐ 有 ☒ 無

・サービス提供への影響、想定される最大リスク 等

「有」が「無」のどちらかにチェック

(3) 事実経過(時系列)

10/5 10:00 外部より入会登録HPに異常な数の申請(1分間に約10万件)が行われていることを検知。(※平時は、1日10件程度)
10/5 10:10 サイバー統括部とシステム担当部署で情報共有を行い対策を検討
10/5 10:26 一時的に当該HPへのアクセス遮断を実施
10/5 13:30 DDoS攻撃事案共通様式を用いて〇〇へ第1報を送付
10/5 14:00 HPを復旧
10/10 18:20 外部より入会登録HPに異常な数の申請(1分間に約15万件)が行われていることを検知。
10/10 18:30 サイバー統括部とシステム担当部署で情報共有を行い対策を検討
10/10 18:30 一時的に当該HPへのアクセス遮断を実施
10/10 20:40 DDoS攻撃事案共通様式を用いて〇〇へ第2報を送付

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し、別紙を別ファイルで添付の順で対応

3. 影響のあるシステム(強化法第5条による報告の場合、特定侵害事象等が発生した特定重要電子計算機について記載)

- ・〇〇株式会社の入会登録HP
- ・システムの稼働状況(一時停止中)

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し、別紙を別ファイルで添付の順で対応

4. 事案に関する技術的な事項（攻撃技術情報）

※記入可能な項目を記載してください。また、間隔を空けて別種の攻撃（波）がある場合は、攻撃（波）毎に本項目を作成することも可能。

（１）観測期間

攻撃開始：	10月	10日	18時	20分	24時表記で記載。特記事項があれば記載
攻撃収束：	10月	10日	21時	30分	
特記事項：					

（２）攻撃類型

①分類（複数選択）（※選択肢は、MITRE ATT&CKのTechniquesを参照しています。）

- ☒ ネットワークへのサービス拒否攻撃 Network Denial of Service (T1498)
※以下に記載のT1498-001又はT1498-002のいずれに該当するかが不明な場合
- ☐ ネットワークへのフラッド攻撃（UDPフラッド攻撃等） Direct Network Flood (T1498-001)
- ☐ ネットワークへのリフレクション攻撃（DNSリフレクション攻撃等） Reflection Amplification (T1498-002)
- ☐ エンドポイントへのサービス拒否攻撃 Endpoint Denial of Service (T1499)
※以下に記載のT1499-001からT1499-004までのいずれに該当するかが不明な場合
- ☐ OS枯渇フラッド（TCPステート枯渇攻撃等） OS Exhaustion Flood (T1499-001)
- ☒ サービス枯渇フラッド（HTTPフラッド攻撃等） Service Exhaustion Flood (T1499-002)
- ☐ アプリケーション枯渇フラッド Application Exhaustion Flood (T1499-003)
- ☐ アプリケーション又はシステムの脆弱性悪用によるサービス妨害攻撃 Application or System Exploitation (T1499-004)

- ☐ その他（ ）
- ☐ 不明

複数選択可。該当項目が無い場合は、「その他」にチェックしたうえで、カッコに内容を

②詳細

(例：DNSサーバに対するランダムサブドメイン攻撃、http Flood攻撃 等)

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の

（３）通信プロトコル

(例：TCP/UDP/ICMP/NTP/HTTP/HTTPS/BGP 等)

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の

（４）送信元情報

- ・送信元のIPアドレス
- ・送信元のポート番号
- ・送信元の機器・ボットネットワーク

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

（５）送信先情報

- ・送信先のIPアドレス
- ・送信先のポート番号
- ・標的とされている機器・アプリケーション 等

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

（６）通信量

(例：10Gbps, 1000pps, 1万RPS 等)

簡潔に記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応

※送信元IPアドレスなど、記載内容が多数になる場合は別ファイルで御提出ください。

5. 事案への対応に関する事項

(1) 公表の実施状況

事案の公表：☒ 実施済

【公表日：2026 年 10 月 5 日】

公表URL：<https://...../news/261005.html>

公表の方法：☒ ホームページに掲載

☐ 実施予定

☐ 検討中

☐ 予定無し

☐ 記者会見

☐ 報道機関等への資料配付

☒ その他：（公式SNSに掲載）

公表文：

公表の方法は、実施済または実施予定のすべての公表方法についてチェック(1回目に記者会見、2回目にホームページ掲載の場合、両方にチェック。公表文については、記者会見の場合には報道関係者への連絡文や会見内容が分かる資料を別様式にて添付、ホームページに掲載の場合には、

(2) 今後の予定

☒ 事象継続中

☐ 対応策を継続中

☐ 対応完了

今後の予定は、いずれかの項目をチェック。「事象継続中」とは「続報がある場合」にチェックを入れる。「対応策を検討中」とは「続報が無い」が対応策を検討している場合にチェックを入れる。すべての対応が終了している場合には「対応完了」にチェック

(3) 外部機関による調査の実施状況

☐ 実施済又は実施中

☐ 実施予定

☒ 検討中

☐ 予定なし

(詳細：

外部機関による調査の実施状況は、いずれかの項目をチェック。チェックした項目に対して、詳細があればあわせて詳細欄に記載

6. その他特記事項

これまでの項目で記載できない内容(特記事項等)があれば記載。セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおりに」と記載し別紙を別ファイルで添付、の順で対応すること。スクリーンショット等を貼り付けることも可